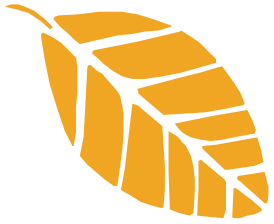


matasano

# Hacking Capitalism
# Exploring Financial Services Protocols

# Agenda

- What are we talking about?
- Elemental Pieces
- Key Protocols
- General problems
- Tools for testing

# What are we talking about?

- Finance runs on a different set of standards than everyone else
  - HTTP/HTTPS dominates in the normal world for “general” application use
  - Finance world is made up of all sorts of weird protocols
- The protocols aren’t as thoroughly beaten up as everything else
  - Financial protocols aren’t general use
  - You can’t build a network at home
    - *Ok that’s a lie, you can…*
  - Their use isn’t obvious
    - *And they all seem to do the same thing*
    - *But differently*

# State of the finance protocol world

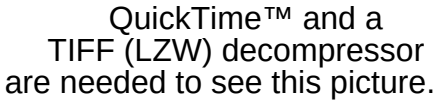
- Design goals
  - Availability
  - Availability
  - Availability
- General protocols
  - Assumed to be running over private networks
  - Encryption often provided by external sources
    - *Stunnel*
    - *VPN*
    - *PGP (Yeah, no joke!)*
  - Where string encryption is possible, its slow

matasano

# Building Blocks

- All sorts of odd protocols
  - The SoupTCP
  - Rendezvous
  - Smart Sockets

# Example: The SoupTCP




- Super simple protocol
- Handful of packet types
- Quick punchlines
  - Login request uses a cleartext username and password
  - Password is case insensitive alphanumerics of 10 chars or less, padded with spaces
  - Sequenced, but sequence can be guessed
  - Only TCP sequence numbers prevent simple teardown attacks

# Key Protocols

- Lots of protocols with funny acronyms and capital letters
  - FIX
  - QIX
  - OUCH
  - OTTO
  - RASHport
  - DROP
  - CTCI
  - ITCH
- For more information: http://www.nasdaqtrader.com

# FIX: Financial Information Exchange

- Complicated protocol
  - Runs over TCP
  - Session Layer Protocol Plus FIXML messages
  - Over 1000 pages of specifications (as of FIX 5.0)
  - Security concerns barely mentioned
- Here are your encryption options:
  - None / Other
  - PKCS (Proprietary)
  - DES (ECB Mode)
  - PKCS / DES (Proprietary)
  - PGP / DES (Defunct)
  - PGP / DES-MD5
  - PEM / DES-MD5

# FIX: Authentication

- Username and password based
- On many systems the passwords never change
  - These passwords are often like
- On a frightening number of systems, there are no passwords
  - Logging in just requires guessing a SenderCompID (Think username)

# Assessing Financial Apps

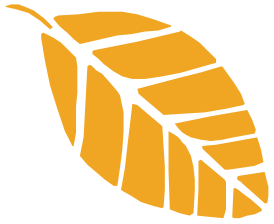
- What the CIA Triad means here:
  - Availability.  Not being able to execute trades can be disastrous.
  - Confidentiality.  Just knowing what transactions are occurring is enough for a well funded entity to profit.
  - Integrity.  Changing transaction amounts is obviously bad.  But it is likely to get caught on the backend.

# Assessment Methodology

- Security 101
  - Are you doing session layer encryption?
  - Are you using passwords?
  - Are you changing passwords?
  - Has that system been patched in the past 5 years?
- Security 102
  - Test Implementations
  - Fuzz for the standard cruft (lots of C and C++ here)
  - Test protocol logic bugs (what can I do pre-authentication?)
  - Test application logic bugs (All hail the BBS time bank withdraw negative time trick)

# References

- FIX Specifications
  - http://www.fixprotocol.org/
- Open Implementations
  - http://www.quickfixengine.org/
- NASDAQ Protocols
  - http://www.nasdaqtrader.com/



matasano

# Questions

Your way of proving you listened…